RECEIVED
CENTRAL FAX CENTER

NOV 27 2006

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0551-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P496/01.134.01

I hereby certify that this correspondence is being transmitted via facsimile to the Commissioner for Patents, Alexandria, VA 22313-1450 to fax number (571) 273-8300.

on November 27, 2006

Signature: Erica L. Farlow

Typed or printed name: Erica L. Farlow

Application Number	Filed
10/025,572	12/26/2001

First Named Inventor: Lee Codel Lawson Tarbotton

Art Unit	Examiner
2131	Zia, S.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Kevin J. Zilka
Typed or printed name

(408) 971-2573
Telephone number

November 27, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

REMARKS

The Examiner has rejected Claims 1-27 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner argues 'that the term "more thorough" in Claims 1, 9, and 17 is a relative term.' In response, applicant respectfully asserts that the following claim language is to be read according to the plain and ordinary meaning thereof, in view of relevant dictionary definitions (see definition(s) presented in Amendment B filed 05/15/06), etc.

The Examiner has also noted that the terms "the computer system" and "the user" in Claim 28 lack sufficient antecedent basis. In response, applicant directs the Examiner's attention to applicant's Claim 1, from which Claim 28 depends, which claims "when an associated **computer system** is at least substantially idle" and "being accessed by a **user**" (emphasis added). Additionally, the Examiner argues that "[t]he term 'least substantially' in claim 1, 9, and 17 is a relative term." Applicant respectfully asserts that the claimed "at least substantially" in all of the pertinent claims is to be read with regards to its plain and ordinary meaning, as evidenced by dictionary definitions, etc. For example, one dictionary definition of "substantial" includes "[c]onsiderable in importance, value, degree, amount, or extent" (*The American Heritage® Dictionary of the English Language, Fourth Edition*).

The Examiner has rejected Claims 1, 8, 9, 16, 17, 24, and 27-28 under 35 U.S.C. 103(a) as being unpatentable over Cozza (U.S. Patent No. 5,502,815), in view of Chess et al. (U.S. Patent No. 6,772,346), in view of Hruska (Virus Detection), and in further view of Ellenberger (U.S. Patent No. 5,684,875). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on item 58 "no" and item 62 in Figure 4 of Cozza to make a prior art showing of applicant's claimed technique where "if no computer files containing malware are found in said storage location, then identifying said storage location as a clean storage location" (see this or similar, but not necessarily identical language in the independent claims). Applicant respectfully asserts that the cache file technique disclosed by Cozza in Figure 4 simply does not meet applicant's claimed "clean storage area." With reference to Figure 4, Cozza teaches that "[i]f no viruses were found in the file, then the file's scan information is added to the new cache in step 62" (Cozza, Col. 5, lines 1-3). In this excerpt, Cozza describes a method of updating a cache file if there are not any viruses found in

the file. If all files were virus free, for example, the cache would contain information on every file. However, having a complete file cache does not imply that the entire cache represents "a clean storage location," as claimed by applicant. In particular, the file cache, as disclosed by Cozza, operates on individual files whereas applicant claims "clean storage locations" (emphasis added), as claimed by applicant.

In the Office Action mailed 07/27/2006, the Examiner has failed to respond to applicant's arguments with respect to applicant's claimed technique where "if no computer files containing malware are found in said storage location, then identifying said storage location as a clean storage location." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

In addition, with respect to the independent claims, the Examiner has relied on item 40 in Figure 4 of Cozza to make a prior art showing of applicant's claimed technique of "... subsequently reading a computer file, [and] determining whether or not said computer file is stored within a clean storage location ..." (see the same or similar, but not necessarily identical language in the independent claims - emphasis added). Applicant's arguments made on page 10, second paragraph of Amendment B mailed 05/15/2006 are hereby incorporated by reference.

In the Office Action mailed 07/27/2006, the Examiner has argued that Cozza "teaches a system and method that relates to storing initial state information concerning the file or volume which is being examined for a virus" and that "[t]his information is stored in a cache in a non-volatile storage medium and when files are subsequently scanned for viruses, the current state information is compared to the initial state information stored in the cache." Further, the Examiner has argued that "[i]f the initial state information differs from the current state information then the file or volume is scanned for viruses which change the state information of the file or volume," and "[i]f the initial state information and current state information is the same then the file or volume is scanned for a subset of viruses which do not change the state information."

Applicant respectfully disagrees with the Examiner's arguments. Specifically, applicant respectfully points out that Cozza teaches that "initial state information concerning the file or volume which is being examined for a virus" is "stored in a cache in a non-volatile storage medium" (Abstract – emphasis added) and that "[f]or each file on a volume that is to be scanned,

the cache is searched for the presence of the file's cache information in step 40" (Col. 4, lines 18-20 – emphasis added). However, merely scanning files in a volume by searching a cache which contains initial state information does not disclose "determining whether or not said computer file is stored within a clean storage location" (emphasis added), as claimed by applicant. Clearly, storing initial state information for a file or volume in a cache fails to suggest that the "computer file is stored within a clean storage location," (emphasis added), in the manner as claimed by applicant.

Further, with respect to the independent claims, the Examiner has relied on items 320, and 330 in Figure 3 of Chess to make a prior art showing of applicant's claimed technique where "if said computer file is not stored within a clean storage location, then malware scanning said computer file" (see the same or similar, but not necessarily identical language in the independent claims). Applicant's arguments made on page 11, second paragraph of Amendment B mailed 05/15/2006.

In the Office Action mailed 07/27/2006, the Examiner has argued that "Chess clearly teaches a specific scanning method as shown in Fig. 3," that "Chess teaches data fork scanning," and that "Chess et al. teach[es] a particular scanning method, which provides 'rigorous analysis...'" as shown in Col. 6, lines 45-55. Applicant respectfully disagrees and asserts that the excerpts in Chess relied on by the Examiner merely teach that a "file is subjected... to rigorous analysis" (Col. 6, lines 45-46) and "is determined... to be either non-malicious... or to contain a new and now-known malicious-code entity" (Col. 6, lines 57-60). However, performing analysis on a file in order to determine if it is malicious, as in Chess, does not teach a technique with a specific condition where "if said computer file is not stored within a clean storage location, then malware scanning said computer file" (emphasis added), as claimed by applicant.

Additionally, applicant notes that the Examiner has also relied on Fig. 4, items 40 "no" -> 42 -> 44 of Cozza to make a prior art showing of applicant's above claimed technique. Applicant respectfully asserts that the excerpts relied upon by the Examiner merely teach that "[f]or each file on a volume that is to be scanned, the cache is searched for the presence of the file's cache information in step 40" (Col. 4, lines 18-20 – emphasis added) and that "[i]f the file's information is not found... then it is scanned for a full complement of viruses, including those that infect the file resource fork in step 42 and those that infect the data fork in step 44" (Col. 4, lines 24-28 – emphasis added). Applicant respectfully notes that scanning a file for viruses if the file's

information is not found in the cache does not teach a technique where "if said computer file is not stored within a clean storage location, then malware scanning said computer file" (emphasis added), as claimed by applicant. Clearly, not finding a file's cache information in a cache fails to meet applicant's claimed "file is not stored within a clean storage location," in the manner as claimed by applicant.

Still yet, with respect to the independent claims, the Examiner has relied upon the Ellenberger reference to make a prior art showing of applicant's claimed technique "wherein said step of malware scanning all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user" (see the same or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the Ellenberger reference merely teaches a method of randomly selecting a mix of fast execution and slow execution virus detection algorithms for each scan (Col 5, lines 25-29). Ellenberger does not teach applicant's claimed technique "wherein said step of malware scanning all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user" (emphasis added), as claimed by applicant. Ellenberger simply does not even mention using different scanning options for background task scanning versus on-access scanning, as claimed.

In the Office Action mailed 07/27/2006, the Examiner has argued that "Ellenberger teaches a virus scanning method where one or more virus detection algorithms are selected at random for each scan." Applicant respectfully disagrees with the Examiner's argument and again respectfully points out that this random selection of virus detection algorithms does not teach applicant's claimed technique "wherein said step of malware scanning all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user" (emphasis added), as claimed by applicant. Clearly, a random selection, as disclosed by Ellenberger, fails to suggest that "a background task is performed with more thorough scanning options" (emphasis added), in the manner as claimed by applicant.

Additionally, with respect to the independent claims, the Examiner has relied on page 129, Col. 2 of Hruska to make a prior art showing of applicant's claimed technique "wherein said malware scanning of all computer files stored within a storage location is performed as a background task that occurs as a function of when an associated computer system is at least substantially idle" (see this or similar, but not necessarily identical language in the independent claims). Applicant's arguments made on page 13, fourth paragraph of Amendment B mailed 05/15/2006 are hereby incorporated by reference.

In the Office Action mailed 07/27/2006, the Examiner has simply reiterated that 'on-access scanning "intercepts file open and file close operations" ... hence making it as a background task.' Applicant respectfully disagrees and again asserts Hruska discloses that "[o]n-access scanning involves intercepting *file open* and *file close* operations*, virus checking the file and allowing the file access or execution" (page 129, Col. 2 – emphasis added), which fails to teach a technique "wherein said malware scanning of all computer files stored within a storage location is performed as a background task that occurs as a function of when an associated computer system is at least substantially idle" (emphasis added), as claimed by applicant. Clearly, intercepting file open and close operations during a file open or execution fails to suggest that an "associated computer system is at least substantially idle" (emphasis added), in the manner as claimed by applicant.